When it comes to virtualization platforms, experts say focus first on the services to be delivered.

BY MACHE CREEGER

CTO Virtualization Roundtable, Part II

Last month we published Part I of a CTO Roundtable forum on virtualization. Sponsored by the ACM Professions Board, the roundtable features five experts on virtualization discussing the current state of the technology and how companies can use it most effectively. In this second and final installment,

the participants address key issues such as choosing the most appropriate virtual machine platform, using virtualization to streamline desktop delivery, and using virtualization as an effective disaster-recovery mechanism.

Participants:

Mache Creeger (Moderator): Creeger is a longtime technology industry veteran based in Silicon Valley. Along with being an *ACM Queue* columnist, he is the principal of Emergent Technology Associates, marketing and business development consultants to technology companies worldwide.

Tom Bishop is CTO of BMC Software. Prior to BMC, Bishop worked at Tivoli, both before and after its initial public offering and acquisition by IBM, and also at Tandem Computers. Ear-

lier in his career Bishop spent 12 years at Bell Labs' Naperville, IL facility and then worked for UNIX International. He graduated from Cornell University with both bachelor's and master's degrees in computer science.

Simon Crosby is the CTO of the Virtualization Management Division at Citrix. He was one of the founders of XenSource and was on the faculty of Cambridge University, where he earned his Ph.D. in computer science. Crosby grew up in South Africa and has master degrees in applied probability and computer science.

Gustav. This is a pseudonym due to the policies of his employer, a large financial services company where he runs distributed systems. Early in his career, Gustav wrote assembler code for telephone switches and did CAD/

CAM work on the NASA space station *Freedom*. He later moved over to large system design while working on a government contract and subsequently worked for a messaging and security startup company in Silicon Valley, taking it public in the mid-1990s. After starting his own consulting firm, he began working at his first large financial firm. Seven or eight years later, he landed at his current company.

Allen Stewart is a Principle Program Manager Lead in the Window Server Division at Microsoft. He began his career working on Unix and Windows operating systems as a system programmer and then moved on to IBM, where he worked on Windows systems

a computer hardware and software emulation company.

Steve Bourne is chair of the ACM Professions Board. He is a former president of ACM and Editor-in-Chief of the *ACM Queue* editorial advisory board. A fellow alumnus with Simon Crosby, Bourne received his Ph.D. from Trinity College, Cambridge. Bourne held management roles at Cisco, Sun, DEC, and SGI and currently is CTO at El Dorado Ventures, where he advises the firm on their technology investments.

STEVE BOURNE: So I'm in this small-to medium-size business (SMB) shop. You have just told me that I have to balance out the disk and the network with

Xen technology built in, and is one of HP's embedded hypervisors. It's the perfect mid-market product.

Virtualization today is not a real "market" and will not be until there are multiple independent, economically successful vendors. There is one very successful vendor today, and my hat's off to VMware. However, its success is equivalent to the TCP/IP stack vendors of the early 1990s, before the stack became a commodity. But things are about to change because until now nobody else has played. The change is that the core value proposition is about to become free.

With Microsoft's Hyper-V hypervisor virtual machine (VM) platform current-

Steve Bourne

Mache Creeger

Allen Stewart

integration on Wall Street. After IBM, Stewart joined Microsoft, where for the first six years he worked as an architect in the newly formed Financial Services Group. He then moved into the Windows Server Division Engineering organization to work on Windows Server releases. His primary focus is virtualization technologies: hardware virtualization, virtualization management, and application virtualization. Stewart is a Microsoft Certified Architect and is on the Board of Directors of the Microsoft Certified Architect Program.

Steve Herrod is the CTO of VMware, where he's worked for seven years. Before VMware, Herrod worked in Texas for companies such as EDS and Bell Northern Research. Earlier in his career Herrod attended school with Mendel Rosenblum, the founder of VMware, and then worked for TransMeta,

my CPUs. This is all very complicated. What am I going to do next year?

GUSTAV: If you want to implement high up in the service stack today, you should choose VMware. It's the one vendor that sells a fully integrated solution. If you're an SMB with 20 people, want maximum flexibility, and want a single-vendor solution, it's VMware. Because to Simon's earlier point, right now they're trying to sell cars; they are not trying to sell engines.

SIMON CROSBY: No, SMBs should choose Citrix XenServer, HP ProLiant Select Edition, which is an entirely HP-branded product. It is an integrated virtualization solution that is part of ProLiant Server, entirely packaged and managed by HP VMM (Virtual Machine Manager), which manages Microsoft, VMware, and XenServer today. It's got the bundled HP toolset included, our

ly at \$28 and my company's Xen hypervisor being free, the price of a hypervisor is heading toward free. If you look at HP's embedded hypervisor offering using our product, it is an incredible value proposition. That same product has more functionality than what made VMware their first \$500 million of revenue. While VMware has had the benefit of market lead and brand presence, HP has knocked the value proposition out of the park. Is Citrix with XenServer an independent viable competitor against VMware? Yes, but that's a tough slog. Enabling companies to create alternative products like Citrix XenServer, HP ProLiant Select Edition greatly expands customer choice for a wide range of market needs.

STEVE HERROD: If you're an SMB with one thousand employees or less—and 70% of our customers are what we de-

fine to be SMBs—you don't care if it's Xen, VMware, or Microsoft. You want simplicity, availability, security, and you want something that can be supported by your staff.

ALLEN STEWART: If you're an SMB and already running Windows Servers 2008, you enable Hyper-V, use the same management tools that you have been using, and depend on the management construct to help you beyond the virtualization platform.

In the SMB market, Microsoft has pushed System Center outside of the enterprise to System Center Essentials. If you have a small amount of servers, buy Essentials, and you can inexpensively manage the platform.

existing player. They challenge the OS guys because virtualization separates them from the hardware; the storage guys because storage management for virtualization is done on the host and that threatens the whole Symantec/VERITAS model; and the management players, too.

VMware confronts a lot of entrenched interests and threatens them. So VMware could end up as a systems management play, a storage management play, or a big brain that manages the future data center—and that would threaten Cisco or their competitors. The interesting thing for VMware is where does it go from here? Every step they take threatens an established ven-

us or other large enterprises today, but may at some future date. These are the real bleeding edge, radically thinking folks. One of the things we saw was that people are putting management in the software deployment layer on top of EC2.^a

My advice for SMBs able to tolerate offsite data processing is that management options, possibly from third parties, will be available in the not-too-distant future for EC2 and other cloud models and provide management flexibility similar to solutions from VMware, Veridian, and Xen. Even in the cloud, where you literally care about nothing, third-party vendors will come in to provide common abstractions.

Tom Bishop

Simon Crosby

Steve Herrod

TOM BISHOP: I think that's right. I think you start with what you know, stick with the vendors you know and the technology you know, and it's going to allow you to get the biggest bang for the least cost.

MACHE CREEGER: If you run lots of Oracle would you work backward from Oracle and ask what would work best?

GUSTAV: No, I'd work backward from the OS level you manage because that's really what you're managing. But back to your point of "I'm not worried that there are three hypervisor vendors," companies should worry less about that because hypervisors from all the vendors are slowly but surely providing the same functionality.

SIMON CROSBY: But then it's about virtualization management. As the market leader in a new category, everything that VMware does challenges an

dor in an existing market sector.

TOM BISHOP: SMB players that purchase management software will get it from the virtualization vendors and the rest will do it by hand, which is what they've always done. I am not saying that their management functions aren't important. It's just that the problems to be solved for the SMB market are not big enough, hard enough, and expensive enough for management companies to address.

MACHE CREEGER: Well, what happens to the management business when management companies cede it to virtualization companies on the SMB side and alternatively get squeezed by offerings from the cloud?

GUSTAV: It's a counter-trend. One of the things we do at our CTO event in California is to bring in early-stage companies that have little chance to sell to

As a classic example, one of the things that I'm most interested in virtualizing right now is the desktop. I might actually use Citrix on top of Xen or VMware, or CXD on top of VMware to do that particular function.

The Citrix technology is much better for the presentation layer of virtualization. At the present state of technology, I find VMware's framework for doing physical-to-virtual migrations and similar functions to be better. In addition to that, I may do an application virtualization layer with a Softgrid-like technology.^b

I might use all three major vendors, depending on their strengths, and

a Amazon's cloud product offering—<http://aws.amazon.com/ec2/>.

b http://en.wikipedia.org/wiki/Microsoft_Application_Virtualization/.

match to our needs to create a single integrated desktop—DaaS, or Desktop as a Service: one vendor for the presentation layer, a different one for application virtualization, and a third one for the hypervisor.

The more interesting point is that from an IT management point of view, the hypervisor is getting less and less interesting. Worry less about where you get your hypervisor from and more about where you get your management from. Ask whether the management you need today can be sufficiently provided by your vendor, whether that is the hardware partner, a third-party, or the direct vendor.

Is the Microsoft hypervisor going to perform slightly better with small packet operations than the other competitors? Maybe, but that is just for this release; it's ephemeral. By the time you've installed it, the competitive matrix has changed, so realistically you don't care. It all comes down to the fact that management technologies change slower than hypervisor technologies.

MACHE CREEGER: It's like the TPC^c wars of the early 1990s. Vendors would jockey back and forth after every release, but at some point customers realized that they could not pick a vendor based on who was ahead at any given moment.

It was mentioned that some companies were putting management tools together over the cloud, and that Microsoft is developing a multi-hypervisor management console.

ALLEN STEWART: Microsoft is an established system-management company and look at managing systems holistically. Initially we focused on the workload and were moving the VM based on the performance of the VM. Now we're looking at the workload that's running in the VM and making decisions based on that.

TOM BISHOP: This is the hard part. You want to make the decision based on application behavior, not on VM behavior.

MACHE CREEGER: You want service-level agreements (SLAs).

TOM BISHOP: The problem is that by and large SLAs are not available today.

ALLEN STEWART: And that is totally our focus in the system-management space.

SIMON CROSBY

Virtualization is a feature set, not an objective. It's a technology that we should look at in the same way as compilers or TCP/IP stacks. It's a passing fad. The real benefits will come out of the overall ability to compose and manage an application throughout its life cycle.

TOM BISHOP: All you're going to do is change the problem. Will everybody build all of their applications using Microsoft tools? No. All we've done is change the context in which we address the SLA.

ALLEN STEWART: Actually in the Microsoft Systems Center world, we don't require you to do that any more. We do require that you have some knowledge about the actual application, and ISVs are building in that knowledge. Once you have that knowledge, you can then make decisions based on that knowledge.

MACHE CREEGER: So should we expect that over time vendors will define standards around instrumentation for service-level responsiveness, but that it's going to take a long time to get there?

SIMON CROSBY: I don't think so. Somebody tell me a metric that everybody cares about. Somebody tell me what this means.

TOM BISHOP: It's capacity, throughput, and response level.

ALLEN STEWART: And one of the ways you do that is by standardizing higher up in the stack. When developers are building these applications, this SLA model is composed with the application.

STEVE BOURNE: One of the things that I have heard from the NANOG^d guys (North American Network Operators Group) is that you are nuts if you're running your desktop in a non-virtual-machine environment and visiting random Web sites. So my question is do you see security on the desktop as a model?

SIMON CROSBY: Yes. There are two layers of virtualization that are useful there. One is the isolation between applications and OSs, where applications are streamed to desktops. The other is having separate VMs for different contexts—a VM for a user's personal context, which can be thrown away and restarted again, and another VM for their corporate work.

People like me want applications to work on an airplane. Another category of user is the task worker. I think there's a ton of different technologies that could provide viable solutions but I think it's too early to comprehensively understand which ones apply to specific user categories.

c <http://www.tpc.org/>.

d <http://www.nanog.org/>.

GUSTAV: I think you will see the browser itself evolve into a VM architecture. Ultimately the browser will offer the option of either resetting or keeping state.

SIMON CROSBY: That's absolutely wrong. If your browser is attacked and the OS is compromised you're done for.

GUSTAV: What I'm suggesting is that the browser captures the changes made during the session and, post session, gives the user the option of making those changes go away. This amounts to having an embedded hypervisor in the browser and presenting the user with the option of maintaining or erasing state upon exit.

SIMON CROSBY: And you know what? It wrote to the hard disk. No matter what that application does, I will go to the hard disk and find it. This is one of the first security flaws Amazon found with EC2. Reset at the application level is ineffective, because if I can get to the hard disk, I will find stuff anyway. People see that information goes to the hard disk and will look to see what is there.

Amazon thought they solved it in EC2 by writing to a virtual hard disk, but it's actually stored on some spinning plate of aluminum. The next time I go into the EC2 virtual machine, I can go and search through that virtual hard disk and I will find proprietary information. Resetting at the application level is not going to help. You really do need to think about security throughout the entire architectural stack.

Application-layer virtualization does provide some help. We have an isolation layer along with VMware and Microsoft. Because the application is not installed in the OS it is invisible to the registry and the file system. As a result, changes made by the application do not reach the layer below.

GUSTAV: I actually wasn't saying resetting at the application level. I was saying that that a hypervisor will be embedded in the binary for the browser that you run.

SIMON CROSBY: But even that wouldn't satisfy the guys at the NSA who want you to go and write zeroes to every sector on every disk. It won't solve the problem, which is that you actually wrote real blocks of storage to some real disk somewhere.

TOM BISHOP: Probably the most innovative solution I've ever seen is from

the Lower Colorado River Authority^e (LCRA). They are an organization based in Austin, TX that manages dams. The way they solve this problem is when you come into work in the morning they give you a laptop that has all the applications you want in a base disk image. You may do anything you want during working hours, and at the end of the day you give the laptop back. Overnight the disk is wiped and a new disk image is blasted back onto the laptop. The next day, you come in and start over with a new base image.

SIMON CROSBY: At Citrix we have a model within Xen Desktop where all VMs boot off the same OS golden image and all have the same base applications. To deliver a user-specific model, user-specific applications are streamed into the VM based on the user's roaming profile. This approach minimizes the number of OS images and VMs that need to be stored. Anything that's written to disk by an executing VM is cached locally in the VM and never written back to the hard drive, and all changes are discarded on every reboot. For certain classes of users, such as call center operators, this approach works very well.

TOM BISHOP: The only state that persists is well defined through the set of applications.

SIMON CROSBY: That's right.

STEVE BOURNE: Should IT managers care about people who are accessing the Internet through desktops in their shop? Should they be considering VMs to protect the internal networks of their organizations?

MACHE CREEGER: Virtualization introduces too much complexity to effectively encapsulate all the operating restrictions on a general desktop, because at the end of the day, general desktops are still about applications, writing to the disk, and network transmission to other intelligent entities. Virtualization is just another layer of abstraction; it doesn't change the functional levels at which problems occur.

GUSTAV: Several vendors have streaming desktop products that allow a desktop to be streamed from a server to a client machine. The desktop can be cached—on a USB key, for example—or not cached at all. Desktop streaming is

useful when I want a client machine to be my desktop for now, but afterward I never want to use it again.

One place you might use this is where you want zero footprint. This would include cases where what you have is known to be good but you want to run it on an environment known to be suspect, such as at an airport kiosk or on people's home machines.

MACHE CREEGER: Looking at the example that Simon suggested earlier, can we define sessions in desktop environments so that at some point you can throw everything away and reauthorize the session with a complete blank slate? Wouldn't that solve a lot of security issues?

TOM BISHOP: Yes, but not independent of the application.

SIMON CROSBY: The key question is whether the virtual hard disk itself is stateful or not. Where does the state that I want to keep live? Is it part of the thing that boots?

GUSTAV: Is it persistent state or is it transitory/disposable state?

SIMON CROSBY: Where does my persistent state live and where does the transient state live?

MACHE CREEGER: You have to define "session" and that's a hard thing to define.

TOM BISHOP: Because it varies from application to application.

SIMON CROSBY: And from user category to user category. In my world, I have VMs on my laptop and each of my VMs is independently snapshotted and stored in S3.^f However, the VMs are simply runtime entities. My personal and work data are held separately, mapped into the runtime upon boot, and independently backed up, block for block onto S3. If I lose my laptop on any day, the hard disk is locked and the machine is of no use to anyone else. I purchase a new laptop, and within download time everything I have is back.

I also use Citrix WAN optimization technology to ensure that no block of data ever gets sent over the wire twice. A 24MB Powerpoint file with just a few changes takes less than a second to back up because 99% of the blocks are already backed up and only the differences are sent over the wire.

^f Amazon's Simple Storage Service—<http://aws.amazon.com/s3/>.

^e <http://www.lcra.org/>.

GUSTAV: There's actually a really powerful application that comes with this. Along with day-to-day virtualization stuff is the issue of disaster recovery (DR). Most SMBs make zero investment in DR. Virtualization becomes incredibly cost effective when it has the ability to send VMs to the cloud for access only when needed.

SIMON CROSBY: The benefits are huge and the numbers are very compelling.

GUSTAV: Typical disaster-recovery costs are 2N (twice the cost of the infrastructure). To say that I can go to 1.05N is game changing.

SIMON CROSBY: The great thing about this kind of approach is that the cloud vendor can lose a data center and my data is still there. They can lose two simultaneously and my data is still there.

MACHE CREEGER: The virtualization abstraction enables fungible data-center capacity, much like the power industry, where people can trade excess capacity on the open market.

SIMON CROSBY: That's right, and like the power industry you will have purely financial players, people in the business who know nothing about technology, simply trading capacity back and forth. The first arbitrage players on the cloud are already in business.

GUSTAV: I will take it back to the insurance space. I can buy true insurance. I can pay 2% of the value of my assets today and know I can absolutely run my exact stuff.

MACHE CREEGER: So it's a bulletproof insurance premium.

TOM BISHOP: That's right. It's how you compute and manage risk.

GUSTAV: It's "How do I take my 2N problem down to 0.02N?" It's "How do I take 98% of my DR cost to zero?" That is just a different way of saying "How do I take 49% of my total IT cost to zero?"

SIMON CROSBY: At the same time, the high-end fault tolerance (FT) moves down to a commoditized, value-priced capability rather than a high-end, hardware capability.

GUSTAV: To give you an example of the thinking behind DR, take 9/11. 9/11 was a black swan; it never should have happened. Any statistical model that you build fails when the black swan shows up, and DR is only valuable if it actually works when the black swan shows up.

You are actually building a model that goes past the black swan. The thing about 9/11 that made it even more chaotic than the tragedy of the Trade Center towers coming down was that 12 Broad Street (the lower Manhattan telecom switching station) filled with water. This resulted in no teleco for the southern tip of Manhattan, creating a black swan.

Theoretically the thing that could never happen, which is that every divergent teleco path in southern Manhattan becomes blocked, happened. Many of the problems that are solved in the typical case are not sufficient in the DR case because the normal constraints do not apply.

TOM BISHOP: The number-one conclusion at this one event I attended was that during Hurricane Katrina every company's disaster-recovery plan assumed people could get to work. Every disaster-recovery plan in New Orleans failed because people could not get to work.

SIMON CROSBY: 9/11 was about mortality. Nobody reasons about how to recover from mortal events. At the end of the day, the rational guy in the SMB doesn't deal with that level of risk. If an event like that happens, his business is lost.

GUSTAV: There actually are levels of defined risk. You've got systemic risk. If the counterparty doesn't show up, the entire market cannot function. That's one level of badness. But think about the SMB. There's a stat I've seen recently that says that 70% of businesses that are forced to close for more than a month never reopen. Systematic risk, well priced, is more valuable to the SMB than it is to a large enterprise like my employer.

The counterargument made earlier states that if this business fails, it is cheaper to start a new business than to pay 2N for 10 years. The problem is that we have never been able to present a reasonably priced alternative.

Effectively the SMB owner is self-insured and betting on his own ability. I would say that DR for the SMB is actually a richer market than DR for the enterprise. I think part of the problem is defining the minimum requirement. It doesn't need to be up in the next five minutes; he just needs to know that he can get it working in two or three days

under any circumstances.

TOM BISHOP: One of the things I learned at Bell Labs was that in terms of fault coverage, you got far better results by recovering from failure than you ever got by avoiding it.

SIMON CROSBY: That is right. A recent Stanford research model tells us to assume that computer systems are inherently fragile, humans build bad software, and applications are going to decay and fail. Therefore we should architect our applications so they inherently contain the concept of failure and restart.

MACHE CREEGER: We are almost out of time here. I'd like you all to summarize what the takeaways are and what kind of advice you're going to give to the poor person who's trying to make sense of the world today and how he can move forward.

STEVE HERROD: At the highest level, I think we should all avoid breathing our own exhaust too much. At the end of the day, virtualization is a tool. The goals are to make life better, and particularly for SMBs, to make computing simpler. To make it easy for SMBs is to enable them to operate highly available and securely, and to solve their business problems with their applications.

It is actually about manageability and how to do more and make things run better with less staff. When you're evaluating your workload and products to address it, you should be looking at the overall story, not just at a snapshot. It's really what you are going to be working with day-to-day. I believe that is what we're all trying to focus on. That is certainly what VMware is trying to focus on.

ALLEN STEWART: Think locally but really have your eye on what you're going to do with virtualization moving forward. Someone in the SMB space is typically looking at virtualization to get flexibility, but think about the actual applications, the use cases, and the user profiles to determine why you want to use virtualization in your environment.

Manageability of the environment is really going to be a critical aspect, not just the fact that you're creating a virtual machine. Integrating the stack into your environment is going to be very important from a small business perspective. You need to determine

whether you will need to retrain your staff to integrate virtualization into your environment, and then weigh that against the benefits.

Certainly think about what you're running in your environment. If you're running Windows, think about using Hyper-V and some sort of high-level management construct that doesn't require you to do a large integration effort.

SIMON CROSBY: Virtualization is a feature set, not an objective. It's a technology that we should look at in the same way as compilers or TCP/IP stacks. It's a passing fad. The real benefits will come out of the overall ability to compose and manage an application throughout its lifecycle.

It is the application that IT is charged with delivering and not virtual machines. The sooner we move the debate from virtual machines back to delivering services to end users, the faster people will focus on the tools that will drive them through that application-life cycle process.

TOM BISHOP: I agree with that. IT transformation today is really all about two things: delivering the services that business cares about and doing it as cheaply and efficiently as possible. Virtualization has a role to play in both of those but it's just an enabler; it's not part of the higher level set of objectives. The challenge is how to fold in the capabilities that virtualization provides into a higher level set of mechanisms to enable you to achieve those two objectives. The harder challenge is changing the focus of what IT does and the people who do the work. A large number of IT people still view recovering the database as their job, not delivering business services.

GUSTAV: My definition of good engineering is *ease of removal*, not *ease of implementation*. One of the common characteristics of the available VM platforms is that transitions between them are relatively easy. Physical-to-virtual migrations don't actually depend on *you* being the physical part for them to work. If you were to look today at a physical-to-virtual migration of something that already happens to be in Veridian or VMware or Xen, it's going to work.

Since most of these platforms have quite sophisticated physical-to-virtual

STEVE HERROD

At the end of the day, virtualization is a tool. The goals are to make life better, and particularly for SMBs, to make computing simpler. To make it easy for SMBs is to enable them to operate highly available and securely, and to solve their business problems with their applications.

movements, worry less about whether you are tying yourself to something that you will be stuck with for many years, and worry more about the types of benefits you will gain from its use.

TOM BISHOP: All of the issues we have been discussing are proxies for the fact that we build applications incorrectly. We build applications without regard to how much they cost to own, how much they cost to manage, and their impacts on their operating environments. As you design your infrastructure architectures, a conversation around application life cycle will be far more productive than a discussion around virtualization.

MACHE CREEGER: So what you're all telling me is something I learned in the AI (Artificial Intelligence) business in the early 1980s. AI was considered to be a market, even though I spent a great deal of time telling folks it was just a technology like compilers and file systems. Virtualization is replaying that old script today with the help of a strong media amplifier. Ultimately, just like AI, virtualization will get subsumed into the toolbox of best IT practices.

Folks need to avoid that hype and have confidence that regardless of vendor choice, all the VM platforms will get you where you need to go. They should focus on the services they need to deliver and work backward to the tools and technologies that best match their needs. They should believe that sensible people in the technical management of all these companies are working toward standards that will allow as much interoperability as is practical and that it will progress over time. As people better understand where virtualization fits as a component in an IT architecture, all the products will evolve towards common functionality. The real analysis should be on what management paradigms you choose and, if you are inclined towards a cloud-based platform, evaluating whether virtualization can be an asset in achieving the benefits of that paradigm.

Mache Creeger (mache@creeger.com) is the principal of Emergent Technology Associates, marketing and business development consultants.

© 2008 ACM 0001-0782/08/1200 \$5.00